PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04L 9/08**	**A1**	(11) International Publication Number: **WO 97/24831** (43) International Publication Date: 10 July 1997 (10.07.97)

(54) Title: MULTIPLE CRYPTOGRAPHIC KEY DISTRIBUTION

(57) **Abstract**

A method for generating data encryption keys providing an increased level of security and versatility is provided for use with data communications between a server and a client. According to this method, a Master Key (MK) is stored in a secured area that is inaccessible to external systems. Also stored in this secured area are several Series Numbers (SN). Based on one of several offered mechanisms, an SN is selected. The selected SN is then encrypted by a conventional data encryption algorithm, such as Data Encryption Standard (DES), using the MK. Through use of the MK, the SN is encrypted by the algorithm to generate a Derived Key (DK). The DK is then used in a second conventional data encryption algorithm. This second algorithm is used to encrypt data that is to be exchanged with an external system, or used to authenticate access. It may also be used to generate an electronic signature.
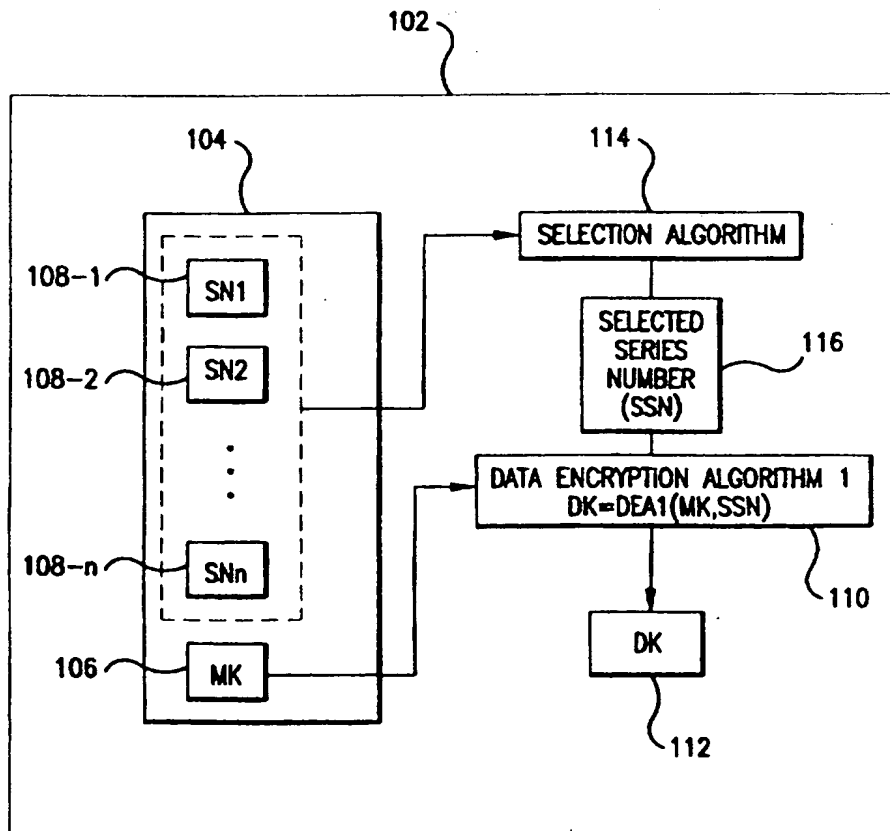
FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic	SD	Sudan
CF	Central African Republic		of Korea	SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

Multiple Cryptographic Key Distribution

Background of the Invention

Field of the Invention

5   The present invention relates generally to computer communications, and more specifically to a means for generating data encryption keys to provide an increased level of data security for communications between a server (such as a computer system) and a client (such as a smartcard).

Related Art

The increased use of computer systems to transmit and receive sensitive
10   data has elevated concerns about data security. For example, recent advancements in computer technology have provided consumer industries with what are commonly known as smartcards. A smartcard resembles a plastic credit card in size, shape, and construction. However, smartcards are essentially computers manufactured on plastic cards. They generally comprise a
15   microprocessor, primary memory, and secondary memory for data storage. Additionally, smartcards have input and output means for exchanging data with external systems. Smartcards store and process application specific data. Commonly, the application specific data is user-specific and pertains to personal and/or business accounts of the smartcard owner.

20   An example of an application of smartcard technology may be found in the banking industry. For example, smartcards may be used to replace common Automated Teller Machine (ATM) cards. Conventional ATM cards merely store data generally used to identify and authenticate users to the ATMs. ATMs typically communicate with central computer systems in order to process requests

by ATM customers. Often, communication line service outages prevent ATMs from processing customer requests.

Smartcards on the other hand, with their built-in active computer circuitry can provide much greater functionality than conventional ATM cards. Smartcards can process data independently of the ATM and the remote computer system. For example, a smartcard that contains current account information such as balance and credit data, may eliminate the need for remote communications between the ATM and the central computer system, thereby decreasing ATM down time. Moreover, smartcards can manage several different accounts at once, and enable transfers and the like between such accounts. For example, people can use their smartcard to pay their credit card bill by issuing a command to transfer funds from their checking account to their credit card account. All information necessary for the transfer is contained within the smartcard itself. Another advantage of smartcards is that they can communicate with several external systems, such as ATM machines, pay phones, and personal computer systems.

Smartcard technology can also be used with telecommunication technology such as wireless telephone communications over cellular networks and other personal communications services (PCS). For example, a smartcard can maintain user account information pertaining to a telecommunication service provider and user specific features. The smartcard, when placed into a slot on a wireless phone, will instruct the phone to send the user's identification and authentication data to the originating switch on the service provider's telephone network. In this way, the telephone network will automatically authenticate the user and access the user's account to provide user-specific and/or system specific features.

A significant consideration in the development and use of smartcard technology is data security. If a smartcard is to be used to access sensitive data regarding a user, certain measures of security are required to protect the user against unauthorized access. Likewise, if sensitive data is to be exchanged

between the smartcard and external systems, data encryption should be implemented.

Smartcards in use today often use data encryption algorithms and encryption/decryption keys. The encryption/decryption keys are commonly multi-
5   bit combinations that enable data encryption algorithms to encrypt data in a predictable manner. The encryption/decryption key is embedded within the permanent memory of the smartcard, and is not accessible by people. Such keys and data encryption methods are used to authenticate the use of the card and to interface with the applications that reside within the external computer systems.
10   Data encryption provides for secure access to user accounts, secure data exchange between the cards and the external systems, and electronic signatures that uniquely and securely identify users to originate smartcard transactions.

If such keys are compromised, the measure of security provided by the key is broken. A key is compromised when it becomes known to an unauthorized
15   user, such as a hacker. A hacker can break the code of a key, for example, with the use of a computer program that rapidly generates numerical combinations and tries each one as a key to gain access to the secured application. Eventually, the right combination is found and the key is broken.

If a smartcard's key is compromised, great expenses are incurred. First, the
20   smartcard must be replaced, since the key is usually hard-coded (permanently coded) into its memory. Even if the key is not hard-coded, the smartcard must still be re-programmed and a new key must be downloaded into its permanent memory storage device. Second, all external systems that communicate with the card must be re-programmed with the card's new key. The cost of such
25   reprogramming and replacement can be very significant.

-4-

Summary of the Invention

A system and method for generating data encryption keys that provide an increased level of security and versatility are provided. The invention is particularly adapted for use with smartcard technology, but is also applicable to other uses, as will be apparent to persons skilled in the art. The present invention stores a Master Key (MK) in a secured area of permanent memory of a device (such as a smartcard), that is inaccessible by humans and systems external to the device. Also stored in this secured area of permanent memory and inaccessible by external systems are several Series Numbers (SN). Based on one of several offered mechanisms, one SN is selected. The selected SN is then encrypted by a conventional data encryption algorithm using the MK to generate a Derived Key (DK). The DK is then used in a second conventional data encryption algorithm. This second algorithm is used to encrypt data that is to be exchanged with an external system, or used to authenticate access. It may also be used to generate an electronic signature.

By using a Derived Key (DK) as an encryption key in a second data encryption algorithm, an additional level of security and versatility are provided. If the DK is compromised, a new DK is generated and the compromised DK is discarded. This occurs through the use of multiple SN's and by altering the mechanism that selects the SNs. The compromised DKs are discarded by software changes only. This eliminates the need for replacing cards and reprogramming external systems with new encryption keys, whenever a key is compromised.

An additional aspect of the present invention relates to its use with conventional Personal Identification Numbers (PIN). The smartcard may be programmed such that the mechanism that selects the SN is the entry of a PIN. Different PIN's will cause the selection of different SNs. If a DK is compromised,

-5-

the user need only enter another PIN. Only the right combination of DK and PIN will cause the external system to authenticate the smartcard.

The smartcard may also be programmed such that multiple sets of Series Numbers (SN) are encoded. This is especially relevant for smartcards that contain

5   multiple applications, such as several credit card accounts. Each set of SN's apply to an individual application or account. A certain PIN will select a corresponding set of SN's that relate to a certain application. Once the appropriate set of SN's is selected, then an individual SN is selected for encryption based on a pre-determined mechanism.

10   Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is

15 .   indicated by the digit(s) to the left of the two rightmost digits in the corresponding reference number.

Brief Description of the Figures

The present invention will be described with reference to the accompanying drawings, wherein:

20   Figure 1 is a block diagram illustrating the architecture of a client such as a smartcard according to the present invention;

Figure 2 is a process flowchart illustrating the general operation of the present invention when used to authenticate client access to a server;

-6-

Figure 3 is a process flowchart illustrating the general operation of the present invention when used to encrypt and decrypt data;

Figure 4 is a process flowchart illustrating the general operation of the present invention, with the additional aspect of utilizing PIN codes; and

5   Figure 5 is a block diagram depicting the architecture of a server that communicates with clients according to the present invention.

Detailed Description of the Preferred Embodiments

Referring to Figure 1, a block diagram of the architecture of a smartcard
10 102 (also referred to herein as "client"), utilizing the present invention is shown. While the invention is described for convenience in the context of a smartcard, it will be appreciated that the invention applies to all applications that use cryptographic keys that are subject to being compromised. To aid simplicity of illustration, components of the smartcard that are not relevant to the invention are
15 not shown. Contained within the smartcard 102 is a secured area of permanent memory 104 that is inaccessible to external systems. A Master Key (MK) 106, and a plurality of Series Numbers (SNs) 108-1 through 108-n, are stored within the secured area 104.   The plurality of Series Numbers are each multiple bit combinations that are permanently programmed into the smartcard 102.

20   External to the secured area of permanent memory 104 is a program that includes a conventional data encryption algorithm (DEA1) 110. This program (DEA1) executes in the smartcard 102. DEA1 110 may be any of several well known standard algorithms used for encrypting data. Details and implementation of such algorithms would be apparent to persons skilled in the relevant art(s). The
25 DEA1 110 receives an input and generates an output. The inputs to DEA1 110

are a selected series number (SSN) 116 and the MK 106. The output of DEA1 110 is a Derived Key (DK) 112.

The selected series number 116 is selected from the plurality of series numbers 108-1 through 108-n. A selection algorithm 114 that is executed by the smartcard 102 is used to select the SSN 116. A unique DK 112 is generated by DEA1 110 for each unique selected series number 116, in combination with the MK 106. Thus, the generation of a Derived Key, DK, is a DEA1 function of the MK and the SSN, such that DK = DEA1(MK, SSN).

Figure 5 is a block diagram depicting the architecture of a server 502 that communicates with clients such as the smartcard 102, according to the present invention. A secured data storage area 504 is used to store a plurality of client information blocks 506-1 through 506-n. Each client information block 506 comprises specific information pertaining to each client 102 that is pre-authorized to communicate and conduct transactions with the server 502.

Each client information block (506-1 through 506-n) includes a plurality of series numbers (such as 1SN ... 1SNn shown in client information block 506-1), and a master key (such as 1MK shown in client information block 506-1). Each client information block stored within the server contains identical data as is stored in the corresponding client's permanent memory area 104. For example, suppose that client information block 506-1, stored within the server 502, corresponds to the client smartcard 102, as shown in Figure 1. In that case, the master key 1MK, shown in client information block 506-1 is the same as the MK 106. Likewise the series numbers, 1SN1 ... 1SNn shown in client information block 506-1, are the same as the series numbers 108-1 through 108-n, stored within the smartcard 102.

External to the secured data storage area 504 is a program that includes a conventional data encryption algorithm (DEA1) 110. This program (DEA1) executes in the server 502. DEA1 110 may be any of several well known standard algorithms used for encrypting data. Details and implementation of such

-8-

algorithms would be apparent to persons skilled in the relevant art(s). The DEA1 110 receives an input and generates an output. The inputs to DEA1 110 are a selected series number (SSN) 116 and master key such as 1MK shown in 506-1. The output of DEA1 110 is a Derived Key (DK) 112.

The selected series number 116 is selected from the plurality of series numbers (1SN1 through 1SNn or example). A selection algorithm 114 that executes in the server 502 is used to select the SSN 116. The unique DK 112 that is generated by DEA1 110, is dependent upon the inputs to the DEA1 110, namely the selected series number 116 and the master key such as 1MK shown in 506-1.

As shown by the use of common reference numbers, the selection algorithms 114 that are executed within the server 502 and the client 102 are functionally equivalent. Therefore both the client 102 and the server 502 will generate the same selected series number, if the same plurality of series numbers are used as inputs to both systems. Likewise, the data encryption algorithms 110 that are executed within the server 502 and the client 102 are functionally equivalent. Therefore both the client 102 and the server 502 will generate the same derived key 112, if the same inputs (namely the selected series number and the master key) are used by both systems.

Note that at least one series number is selected to implement the additional level of data security according to the present invention. Many different methods and/or different algorithms can be used to select a particular series number from the plurality of series numbers according to the present invention. One method is to use the same selection algorithm 114 in both the server 502 and the client 102. In this case, the same SN is selected in both the server 502 and the client 102, since they both use the same algorithm. Alternatively, only one system, either the server 502 or the client 102 uses the selection algorithm. In this case, the output from the selection algorithm is passed to the other system, so that both systems generate common DKs. Several such examples of selection methods are discussed

below in order to demonstrate preferred ways to implement the present invention. In addition to the examples below, many other variations are possible and as such, these examples should not be construed to limit the scope of the present invention.

One method which may be used to select a SN 106 from the plurality of SNs is by using an algorithm 114 programmed within the smartcard 102 that generates a random number. The random number is used as an index to select a particular SN 116. The SSN 116 is subsequently passed to the server 502 in an initialization transaction. The server 502 uses the SSN 116 received from the smartcard 102, along with the MK associated with the smartcard, (1MK shown in client information block 506-1, for example), to generate the same DK 112. The smartcard 102 acts in a similar manner. Accordingly, the transaction is validated.

A variation on the above method is to have the server 502 generate the SSN 116 to be used by both the server 502 and the smartcard 102. The same or similar random number generating algorithm 114 as described above resides in the server 502. The selection algorithm 114 is used by the server 502 to select a SN from the plurality of SNs (1SN1-1SNn, for example) contained in the information 506-1 block corresponding to the smartcard 102, thereby generating a SSN 116. The SSN 116 is used by the server 502, along with the MK associated with the smartcard 102 (1MK shown in client information block 506-1, for example), to generate a DK 112 for the current transaction. The SSN 116 is passed to the smartcard 102, where along with its internal MK 106, generates the same DK 112 via the DEA1 110 in the smartcard 102, thus validating the transaction.

Another example is to have the same selection algorithm 114 execute in both the client 102 and the server 502. The common algorithm 114 generates an index based on a non-random figure, such as date or the time. The index is then used by both the client 102 and the server 502 simultaneously to select a SSN 116, and generate a DK 112 for the session, as previously discussed herein. Alternatively, this non-random type algorithm may be programmed within only

one of the systems and the SSN is passed to the other system, as described above, for example, in an initialization transaction.

A secret code that is assigned to a smartcard holder, commonly referred to as a Personal Identification Number (PIN), can be used to select a particular SN. Such a number for example, can be used as an index to select a SN, or can be used as input to any number of different algorithms which are used to generate an index for the SN selection.

As can be seen, many different methods for SN selection are available and will work as long as the same procedure is used in both the smartcard 102 and the server 502, or the actual SN 116 is passed from one system to the other. In this way, the SSN 110 that is used by the smartcard 102, as input to its DEA1 110, is identical to the SSN 110 used by the server 502, as input to the server's DEA1 110, so that identical DKs 112 are generated by both systems.

Referring now to Figure 2, a process flowchart illustrates the general operation of the present invention when used to authenticate client access to a server. In this example, the client may be a smartcard and the server may be a bank's ATM. The process begins in step 202, where the client requests access to the server. In step 204, the server passes token 205 to the client. The token 205 is subsequently used as input during a data encryption step 212a performed by the server and a data encryption step 212b performed by the client. Token 205 is simply a number that will be used by both the server and the client during data encryption step 212a and 212b, and must be the same for both to authenticate access. The passing of the token in step 204 does not necessarily have to occur at this point in the process but should occur prior to steps 212a and 212b.

The processes continues within both the client and the server whereby each system generates a derived key. Such processes occur in parallel within the client and the server. Steps 206a through 212a depict the process steps taken by the server and steps 206b through 212b depict the process steps taken by the client.

The server process begins with step 206a. In step 208a, the mechanism that selects the SSN 116 is executed. As previously discussed, this mechanism is typically an algorithm such as selection algorithm 114 that generates an index number n, which is used to specify the SN to be used for the current transaction.

5 Other methods to select a SN could alternatively be used. The SSN 116 is made known to the client, by either passing the SSN 116 to the client, or by running the same or similar algorithm in the client as previously discussed herein, such that the client generated SSN 116 is the same as the server generated SSN 116. The method used by the client and the server is defined before the processing of the

10 flowchart of Figure 2. Such definition may be achieved via an initialization transaction between the server and the client.

The SSN 116 is used as input to step 210a, which is the first Data Encryption Algorithm (DEA1), as previously described. A second input to DEA1 210a is the MK 106, which is common to and stored in both the client and server,

15 as previously discussed. In step 210a, DEA1 uses the SSN 116 and the MK 106 to generate the derived key (DK) 112 to be used in the current transaction. A similar process for generating the same DK 112 executes in the client in steps 206b through 210b.

In both the client and the server, the derived key 112 is used in a second

20 Data Encryption Algorithm (DEA2) in steps 212a and 212b to encrypt the token 205. DEA2 may or may not be the same encryption algorithm used in DEA1. As noted above, DEA1 and DEA2 are any well known encryption algorithm. The token 205 is a common number to both the client and server. Therefore, identical results (214a and 214b) are obtained from the server's DEA2 212a and the

25 client's DEA2 212b.

The client result 214b is passed to the server in step 216. The server receives the client result 214b in step 218. In step 220, the server compares the client result 214b with the server result 214a. If the client result 214b matches the server result 214a, then the server allows access, as indicated by step 222. If

the client result 214b does not match the server result 214a, then the server does not allow access, as indicated in step 224.

Referring to Figure 3, a process flowchart illustrates another embodiment of the present invention. In this example, the client may be a smartcard which needs to pass a confidential number N1 304 to a server, which may be an external computer system. In this example, the exchange of N1 304 must be kept secure. Therefore, N1 is encrypted using a Derived Key (DK) 112, as is characteristic of the present invention. The transaction of exchanging the confidential number N1 304 begins with step 302.

Steps 206a through 210a and steps 206b through 210b are the same process steps as shown in Figure 2, used to produce the derived key 112 in the server and client respectively. Note that the token passing step 204 is not used in the process depicted by Figure 3.

The DK 112 that is generated by the client process in step 210b is used as a key for a second Data Encryption Algorithm (DEA2) in step 306. DEA2 accepts the number N1 304 as a first input and the DK 112 as a second input. The output of DEA2 is an encrypted number EN1 308, which is passed to the server in step 310.

In step 312, a decryption algorithm, which is the reverse of DEA2, is used to regenerate the confidential number N1. In step 312, the server uses an independently derived DK 112 as a first input and the received EN1 308 as a second input. Using this method, N1 304 is exchanged between the client (smartcard) and the server (external computer system) in an encrypted manner so as to maintain security.

Furthermore, the specific encryption of N1 304 results from the use of a common Derived Key 112, which is independently generated by both the client and server. As with all of the methods described herein, if the DK 112 is compromised, a new DK can be generated by both the client and server by selecting a new SN. A new SN may be selected by using a different selection

-13-

algorithm, or by using the same selection algorithm with different inputs. Accordingly, the present invention effectively removes the compromised DK from use. Many methods may be used to implement the modification of the selection algorithms used by the client and/or the server. For example, both the client and
5   the server may be manually reconfigured, or may be automatically reconfigured via a transaction between the client and the server. Other implementations will be apparent to persons skilled in the relevant art(s).

An additional aspect of the present invention will now be described with reference to the use of Personal Identification Numbers (PINs). PINs are
10   commonly, but not necessarily, four digits in length. The smartcard 102 may be used for several different applications. For example, a single smartcard 102 may contain numerous credit card accounts. It may also contain multiple sets of SN's, where each individual set corresponds to a different application and /or server. An individual set of SNs is selected within the smartcard. A particular set of SN's is
15   selected by the smartcard, as the result of a user entering a particular PIN into the server. Once a particular set of SNs is selected, the same process as previously described above is used within the smartcard and the server to conduct secure transactions. In addition to providing a means of security, this method also provides a means for automatically selecting an application on a multi-application
20   smartcard.

Referring now to Figure 4, this operation of an additional embodiment is illustrated. After the transaction begins in step 302, the server process begins as step 206a indicates. A user inputs a particular PIN into the server, as indicated by step 402. The PIN 404 is passed to the client to be used as input to a series
25   number set selection process within the client. In step 406 a particular set of SN's that corresponds to the particular application, such as an ATM bank account, is selected, in the client, based on the PIN 404. The set of SNs may be similarly selected in the server, as indicated by step 403. The process from this point on, continues in the same manner as previously described, beginning with the SN

selection steps by both the client and the server as depicted by steps 208b and 208a respectively. Either steps 290 from Figure 2 or steps 390 from Figure 3 may be performed, as indicated by step 490.

5   While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

-15-

What Is Claimed Is:

1. 1.   A system for secured data communication between a client and a server
2. comprising:
3.   a client comprising:
4.   a secure memory suitable for storing data that is inaccessible
5. outside of said client;
6.   a master key stored within the secure memory;
7.   a plurality of series numbers stored within the secure memory; and
8.   a first encryption device coupled to said master key and said series
9. numbers, to generate a first derived key from one of said series numbers,
10. and said master key;
11.   a server in communication with said client, comprising:
12.   a server memory device;
13.   a plurality of master keys stored in the server memory device, each
14. master key associated with a particular client that is pre-authorized to
15. communicate and conduct transactions with the server;
16.   a plurality of sets of series numbers stored in the server memory
17. device, each set associated with a particular client that is pre-authorized
18. to communicate and conduct transactions with the server;
19.   a second encryption device, functionally equivalent to said first
20. encryption device, to generate a second derived key from a series number
21. from one of said sets of series numbers in said server memory device that
22. corresponds to said client, and one of said master keys in said server
23. memory device that corresponds to said client, said first and second
24. derived keys being identical.

-16-

1   2.   The system of claim 1, wherein the client further comprises a
2   selecting means for selecting a particular series number from said plurality
3   of series numbers.

1   3.   The system of claim 2, wherein the server further comprises a
2   second selecting means for selecting a particular series number from said
3   set of series numbers that corresponds to said client.

1   4.   The system of claim 3, whereby said second selecting means is
2   functionally equivalent to said first selecting means so that the same
3   particular series number is selected by both said first and second selecting
4   means.

1   5.   The system of claim 2 wherein said selected series number is
2   communicated to the server so that the server may use the same series
3   number as the client.

1   6.   The system of claim 3 wherein said selected series number is
2   communicated to the client so that the client may use the same series
3   number as the server.

1   7.   The system of claim 2 wherein said first selecting means comprises:
2   means for accepting a personal identification number from a user;
3   means for selecting a set of series numbers from said plurality of
4   series numbers based on said personal identification number; and
5   means for selecting a particular series number from said set of
6   series numbers.

1
2

8.   The system of claim 1, wherein said first and second derived keys are used in subsequent encryption processes as encryption keys.

1
2
3
4
5
.6
7
8
9
10
11
12

9.   A method for secured data communication between a client and a server, said client comprising a first encryption device, and a secure memory suitable for storing data that is inaccessible outside of said client, said server comprising a second encryption device and a memory device, said method comprising the steps of:

        (1)   storing, within the secure memory of the client, a master key;

        (2)   storing, within the secure memory of the client, a plurality of series numbers; and

        (3)   using said master key and said plurality of series of numbers by the client to validate and conduct transactions with said server.

1
2
3
4
5

10.   The method of claim 9, wherein step (3) comprises the steps of:

        (a)   selecting, by the client, a particular series number from the plurality of series numbers;

        (b)   generating, by the client, a derived key using said master key and said selected number.

1
2
3
4
5
6
7

11.   The method of claim 10, further comprising the steps of:

        (4)   storing, within the memory device of the server, a plurality of master keys, each master key associated with a client that is pre-authorized to communicate and conduct transactions with said server;

        (5)   storing, within the memory device of the server, a plurality of sets of series numbers, each set associated with a client that is pre-authorized to communicate and conduct transactions with said server;

8   (6)   selecting, by the server, a particular master key from said

9   plurality of master keys, said particular master key being associated with

10   said client; and

11   (7)   selecting, by the server, a particular set of series numbers

12   from said plurality of sets of series numbers, said particular set of series

13   numbers being associated with said client.

1   12.   The method of claim 11, further comprising the steps of:

2   (8)   selecting, by the server, a particular series number from

3   said particular set of series numbers;

4   (9)   generating, by the server, a derived key identical to said

5   derived key generated in step (3)(b), by using said particular master key

6   and said selected series number.

1   13.   The method of claim 12, wherein the selection method of step (8)

2   is functionally identical to the selection method of step (3)(a), so that both

3   the client and the server selects the same said particular series number.

1   14.   The method of claim 10, wherein the client sends the selected

2   series number to the server so that the server may use the same selected

3   series number as the client.

1   15.   The method of claim 9, wherein step (3) comprises the steps of:

2   (a)   accepting a personal identification number from a user;

3   (b)   selecting a set of series numbers from said plurality of

4   series numbers based on said personal identification number;

5   (c)   selecting a particular series number from said set of series

6   numbers; and

7   (d)   generating, by the client, a derived key using said master

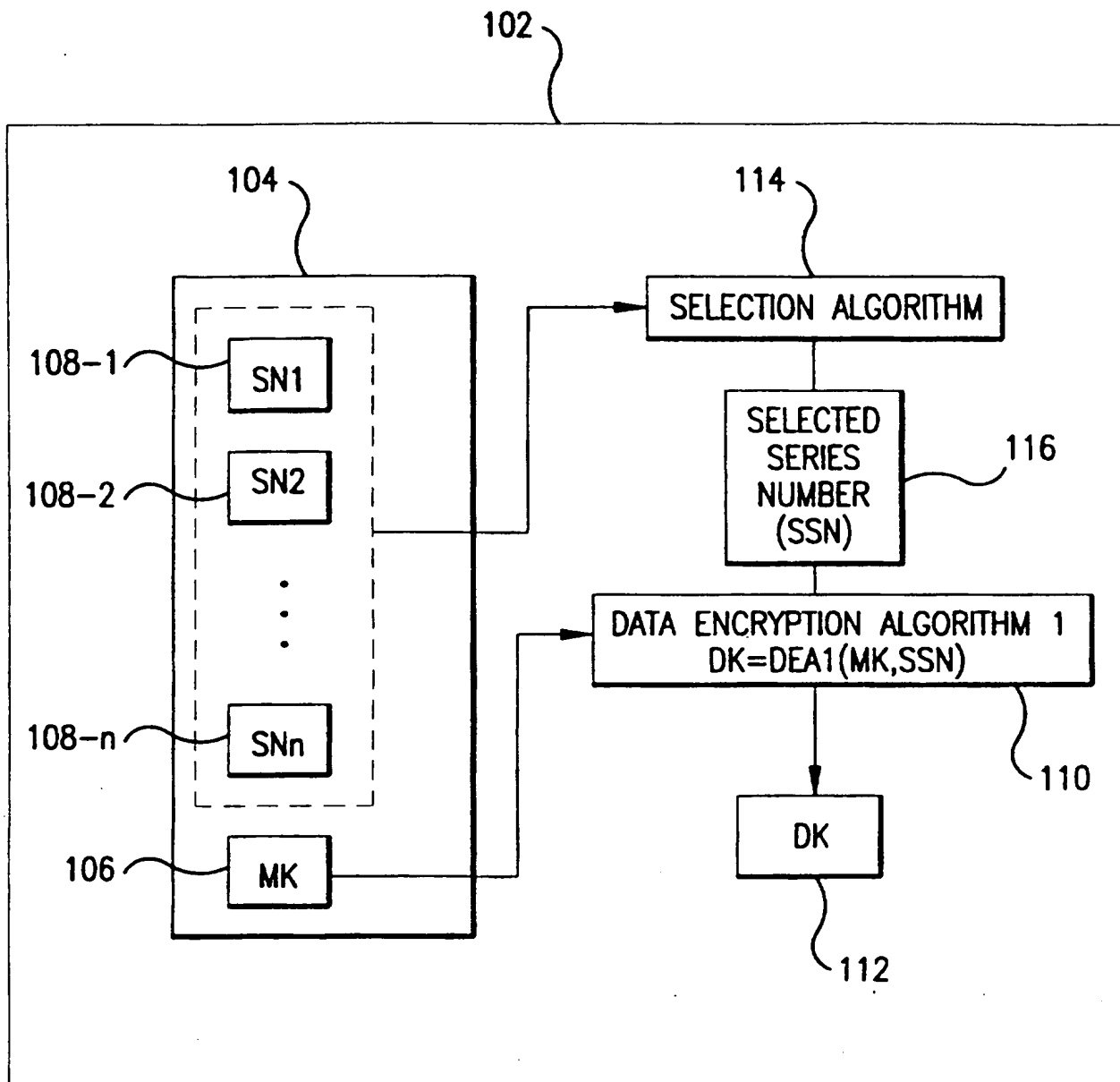8   key and said selected series numbers.

FIG.1

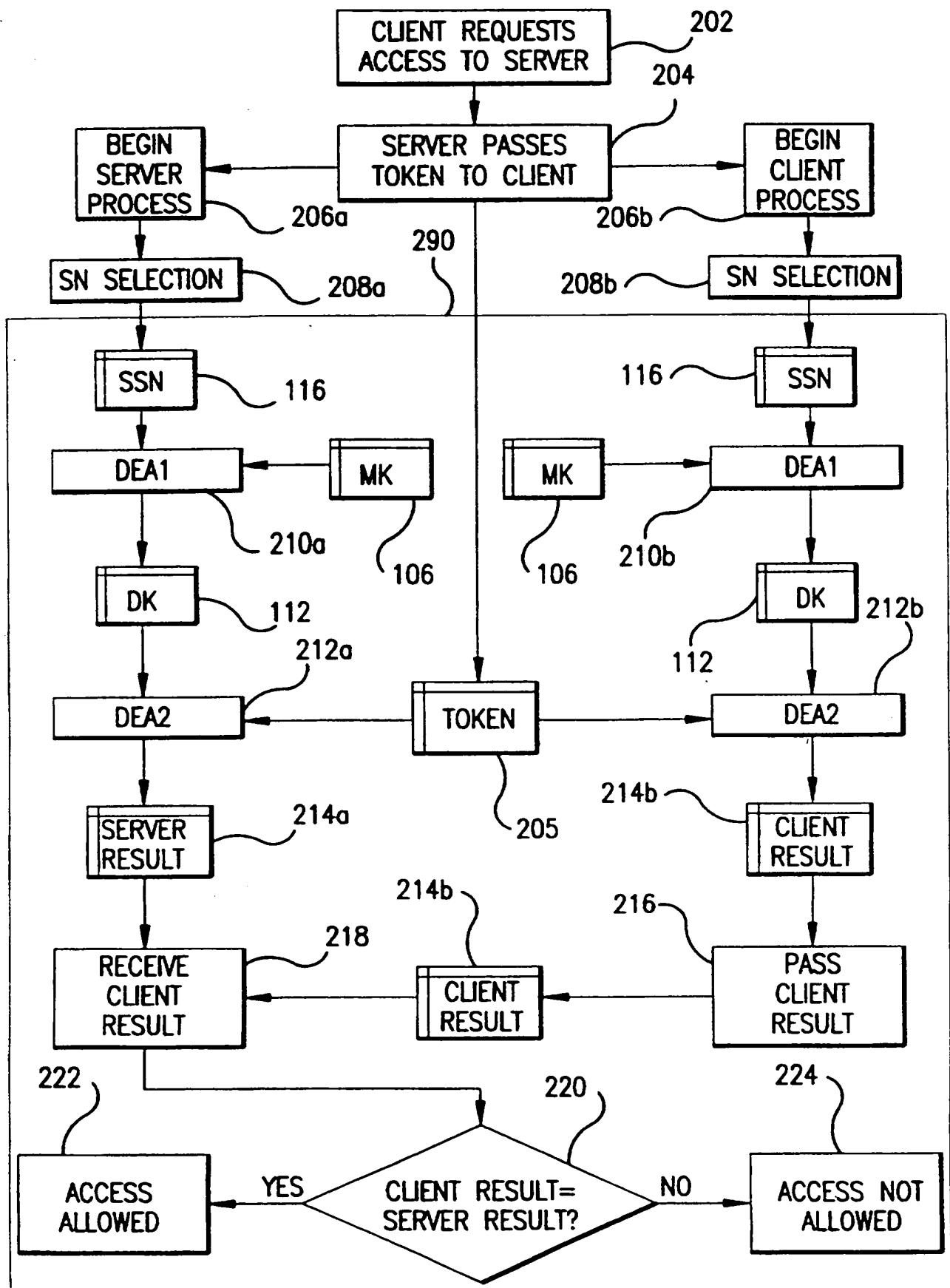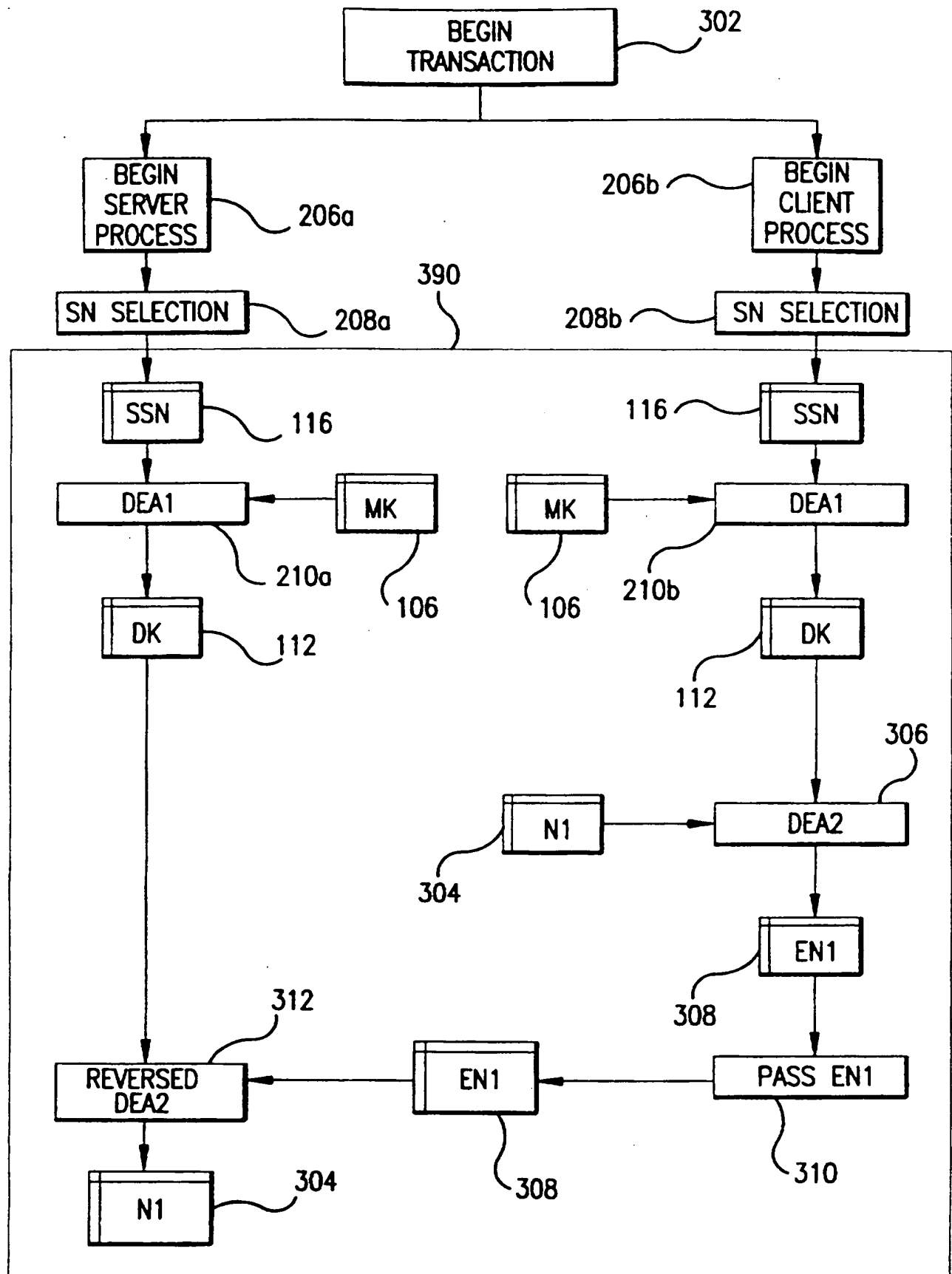FIG.2

3/5

FIG.3
SUBSTITUTE SHEET (RULE 26)

302 BEGIN TRANSACTION

206a BEGIN SERVER PROCESS

206b BEGIN CLIENT PROCESS

402 PIN INPUT

404 PIN

406 SN SET SELECTION

403 SN SET SELECTION

208a SN SELECTION

208b SN SELECTION

STEPS 290 (FIGURE 2)
OR
STEPS 390 (FIGURE 3)

FIG.4

FIG.5

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4935961 A	19-06-90	NONE	
US 5357571 A	18-10-94	AU 663258 B	28-09-95
		AU 6480394 A	27-01-95
		BR 9402606 A	04-04-95
		CA 2126054 A	02-01-95
		CN 1105168 A	12-07-95
		CZ 9401538 A	18-01-95
		DE 4423209 A	19-01-95
		FR 2708403 A	03-02-95
		GB 2279537 A	04-01-95
		PL 304010 A	09-01-95
WO 8102655 A	17-09-81	US 4317957 A	02-03-82
		AU 6929081 A	23-09-81
		CA 1156761 A	08-11-83
		DE 3176872 A	13-10-88
		EP 0047285 A	17-03-82

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 81 02655 A (SENDROW) 17 September 1981 see page 11, line 12 - line 32 -----	1,7,9,15